2017 RMA COMMUNITY BANKS ASSET SIZE: UP TO $10 BILLION THIRD-PARTY RISK MANAGEMENT SURVEY- EXECUTIVE SUMMARY

FINAL REPORT
NOVEMBER 2017

JOIN. ENGAGE. LEAD.

Operational Risk

ACKNOWLEDGMENTS

The 2017 survey was designed with the help of RMA's Vendor Risk Management Steering Committee, comprised of Debbie Manos-McHenry (Huntington Bank), John Klapmust (Bank of the West), Linda Quong (Charles Schwab), and Linda Tuck Chapman (ONTALA Performance Solutions Ltd).

The purpose of the survey was to capture the range of practices in third-party risk management over a cross section of RMA member institutions, and to gather detailed information on current and best practices and challenges in third-party risk management.

The final report provides participants' responses, while protecting the confidentiality of individual institutions by masking the source of the responses.

Note: Due to rounding, percentages in the tables may not add up to 100.

The RMA staff member contributing to the study was Sylwia M. Czajkowska.

Institutions (40) that participated in the survey:

Anonymous
1st National
Adirondack Bank
Amarillo National Bank
American Bank
American National Bank of Texas
Brighton Bank
Broadway National Bank
California Business Bank
CenterState Bank, NA
City Bank
Commercial Bank of Texas NA
Fidelity Bank
First Federal Lakewood
Freedom Bank
Glacier Bancorp, Inc.
Guaranty Bank & Trust
Industrial and Commercial Bank of China (USA) NA
Intrust Bank
John Deere
Lakeland Bank
Los Alamos National Bank

MidFirst Bank
National Bank of Middlebury
NHMB
Park Sterling Bank
Parkside Financial Bank & Trust
Peoples National Bank
Pikes Peak National Bank
Ponce De Leon Federal Bank
Signature Bank
Skagit Bank
State Bank of Cross Plains
Stephenson National Bank & Trust
The Citizens National Bank
TIB
Tioga State Bank
Union Community Bank
WestStar Bank
WSFS Bank

Disclaimer

The information contained herein is obtained from sources believed to be accurate and reliable. All representations contained herein are believed by RMA to be as accurate as the data and methodologies will allow. However, because of the possibilities of human and mechanical error, as well as unforeseen factors beyond RMA's control, the information herein is provided "as is" without warranty of any kind, and RMA makes no representations or warranties expressed or implied to a subscriber or any other person or entity as to the accuracy, timeliness, completeness, merchantability, or fitness for any particular purpose of any of the information contained herein. Furthermore, RMA disclaims any responsibility to update the information. Moreover, information is supplied without warranty on the understanding that any person who acts upon it or otherwise changes position in reliance thereon does so entirely at such person's own risk.

The report is provided to participating institutions for internal analytical and planning purposes only. As such, a participating institution may disclose the information to consultants and agents that are engaged to assist that participating institution in analysis and planning; however, such consultant or agent is prohibited from using the information for any purpose other than such analysis and planning for that participating institution.

About RMA

The Risk Management Association (RMA) is a not-for-profit, member-driven professional association serving the financial services industry. Its sole purpose is to advance the use of sound risk management principles in the financial services industry. RMA promotes an enterprise approach to risk management that focuses on credit risk, market risk, operational risk, securities lending, and regulatory issues. Founded in 1914, RMA was originally called the Robert Morris Associates, named after American patriot Robert Morris, a signer of the Declaration of Independence. Morris, the principal financier of the Revolutionary War, helped establish our country's banking system.

Today, RMA has approximately 2,500 institutional members. These include banks of all sizes as well as nonbank financial institutions. RMA is proud of the leadership role its member institutions take in the financial services industry. Relationship managers, credit officers, risk managers, and other financial services professionals in these organizations with responsibilities related to the risk management function represent these institutions within RMA. Known as RMA Associates, more than 18,000 of these individuals are located throughout North America and financial centers in Europe, Australia, and Asia.

Members actively participate in the RMA network of chapters. These chapters are run by RMA Associates on a volunteer basis and they provide our members with opportunities in their local communities for education, training, and networking throughout all stages of their financial services career. Chapters are located across the U.S. and Canada as well as in global financial centers.

RMA members also avail themselves of benefits offered through headquarters in Philadelphia, Pennsylvania. To assist members in advancing sound risk management principles, RMA keeps members informed and provides access to industry information at this site; publishes *The RMA Journal* and a variety of newsletters, books, and statistics; conducts workshops and seminars; holds conferences, including an annual convention (Annual Risk Management Conference); and has numerous committees working on a variety of projects.

Visit RMA at www.rmahq.org.

Note: As a not-for-profit, professional association, RMA does not lobby on behalf of the industry.

EXECUTIVE SUMMARY

The survey was conducted by The Risk Management Association (RMA) between June and August 2017. Most of the questions were multiple choice with opportunities to provide comments. Some questions were open text, designed to provide information and insight about best and current practices.

A total of 40 responses from large and regional size banks were received, covering a range of asset sizes up to $10 billion. This year, RMA decided to conduct separate surveys for mid-tier banks, large and regional banks, and community banks.

Participating institutions were asked to provide their primary regulator for context and further analysis. As expected, all participating institutions are regulated by one or more of the following: OCC, FRB, and FDIC.

The following areas were addressed in the survey:

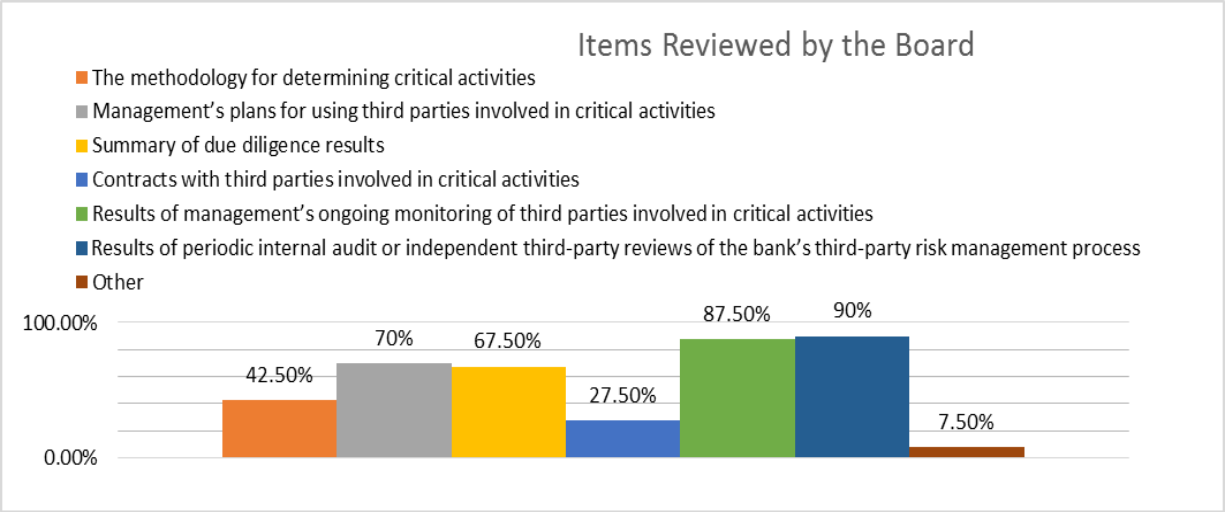
1. Third-Party Risk Management Framework.
2. Third-Party Selection and Monitoring Process.
3. Critical Third-Parties and Critical Activities.
4. Tools and Technology.
5. Contracts.
6. Regulatory and Compliance.
7. Fourth Parties.

Some questions were repeated from the 2014 and 2015 baseline surveys. This will help financial services companies track their progress and evolution of practices.

Third-Party Risk Management Framework

When asked about the Board of Directors' involvement with third-party risk management, a majority of institutions (>87%) confirmed that their Board ensures that strategies related to the bank's core competencies appropriately address which services to retain and which services to outsource to third parties. Key items reviewed by the Board include (in the order of highest responses):

- Results of periodic internal audit or independent third-party reviews of the bank's third-party risk management process.
- Results of management's ongoing monitoring of third parties involved in critical activities.
- Management's plans for using third parties involved in critical activities.
- Summary of due diligence reports.
- The methodology for determining critical activities.



For more than 90% of respondents, the institution's overall strategy for third-party risk is well understood and fully aligned with the institution's overall risk appetite.

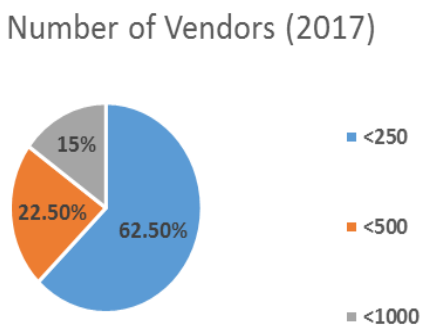
Third-party risk management programs are evolving quickly. In the 2014 survey, 0% of respondents described their "vendor" third-party risk management program as fully mature. In the 2015 survey, 40% indicated that their program is fully mature and 37% of participating institutions reported that their program will be fully mature in less than a year. In this year's data, we see that 52% of participants consider their third-party risk management program to be fully mature and 32% will become fully mature in less than a year.

Response	**2017**	**2015**		**2014**	
Fully mature	52.5%	40%		1-Completely mature	0%
Will be fully mature in less than a year	32.5%	37.8%		2	26.2%
Doesn't address the full lifecycle yet	15%	11.1%		3	49.2%
New or underway	0%	11.1%		4	21.3%
				5-Not Mature at all	3.3%

Since 2014, there has been a shift in how the vendors are managed. About 32% of vendors are managed in the business, compared to 70% in the 2014 survey for the same asset size category.

The composition of the number of vendors within the scope of the program has shifted since our last survey. About 53% of respondents predict that the current number of third parties will increase in the next two to three years and 40% predict that the number of vendors in their program will remain at the same level.

# of Vendors	2017	2015	2014
<250	62.5%	73.3%	67.2%
<500	22.5%	20%	19.7%
<1,000	15%	4.4%	8.2%
<1,500	0%	0%	1.6%
<2,000	0%	0%	0%
<2,500	0%	0%	0%
>2,500	0%	2.2%	3.3%



For institutions with asset size up to $10 billion, the number of FTEs supporting related activities has changed from the 2015 survey.

Total # of FTEs	"vendor" third-parties (2017)		FTEs dedicated to: Total # of FTEs	"vendor" third-parties (2015)	"non-vendor" third-parties (2015)
1	52.5%		**<3**	86.7%	91.1%
2-3	40%		**3-5**	8.9%	6.7%
4-5	7.5%		**6-10**	0%	2.2%
6-10	0%		**11-15**	2.2%	0%
>10	0%		**16-25**	2.2%	0%
			>25	0%	0%

Third-Party Selection and Monitoring

The main factor driving the process to identify the third parties that will be actively managed within an institution's third-party risk management program is by products/services provided (50% responses). About 37% of respondents selected it as determined by calculator/algorithm built into the third-party risk assessment questionnaire. In the 2015 report, the data was reversed and the responses were 35% and 51%.

About 62% of the participants indicated they send due diligence questionnaires for risk assessment purposes, in addition to the RFP questions. The preferred alternatives to these questionnaires include: SOC (Types 1, 2, and 3), SSAE16 (Types 1 and 2) reports, National Institute of Standards and Technology, and ISO27001 certification.

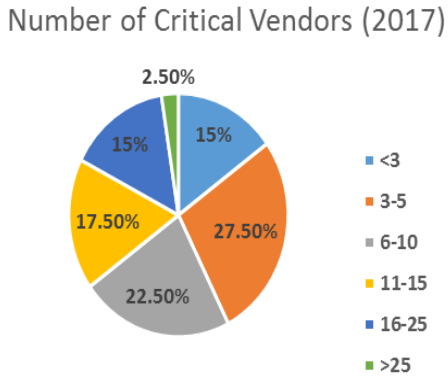
Taking into consideration the amount of work required to review a vendor, 81% of respondents would be willing to consider using a shared assessment provided by a third party.

Critical Third Parties and Critical Activities

Over the years, the number of "enterprise critical" third parties has changed. Consistently, the figures show that the majority of institutions have either between 3 to 5 or 6 to 10

"enterprise critical" vendors—vendors that have the potential to bring the bank to its knees—in their programs.

# of Critical Vendors	2017	2015	2014
<3	15%	8.90%	11.50%
3-5	27.50%	35.60%	18%
6-10	22.50%	37.80%	34.40%
11-15	17.50%	4.40%	19.70%
16-25	15%	6.70%	9.80%
>25	2.50%	6.70%	6.60%



About 25% of respondents conduct site visits for their most and/or high risk critical third parties, while 25% of those who conduct site visits do so on an annual basis. Out of the 25% who conduct site visits, about 38% do not have resources dedicated to this task. The majority of institutions (57%) responded that they do not conduct site visits, but accept independent third-party audit reports in lieu of site visits (e.g., SOC 2).

There is evidence that institutions are gaining clarity around third-party management requirements. For example, definitions of "critical activities" provided in the 2014 report were somewhat vague. The definitions are much more precise in this year's report. Furthermore, the definition of "critical activity" is fully defined for 69% of the institutions who contributed to the study. About 15% are in the process of defining it and about 15% have yet to define it.

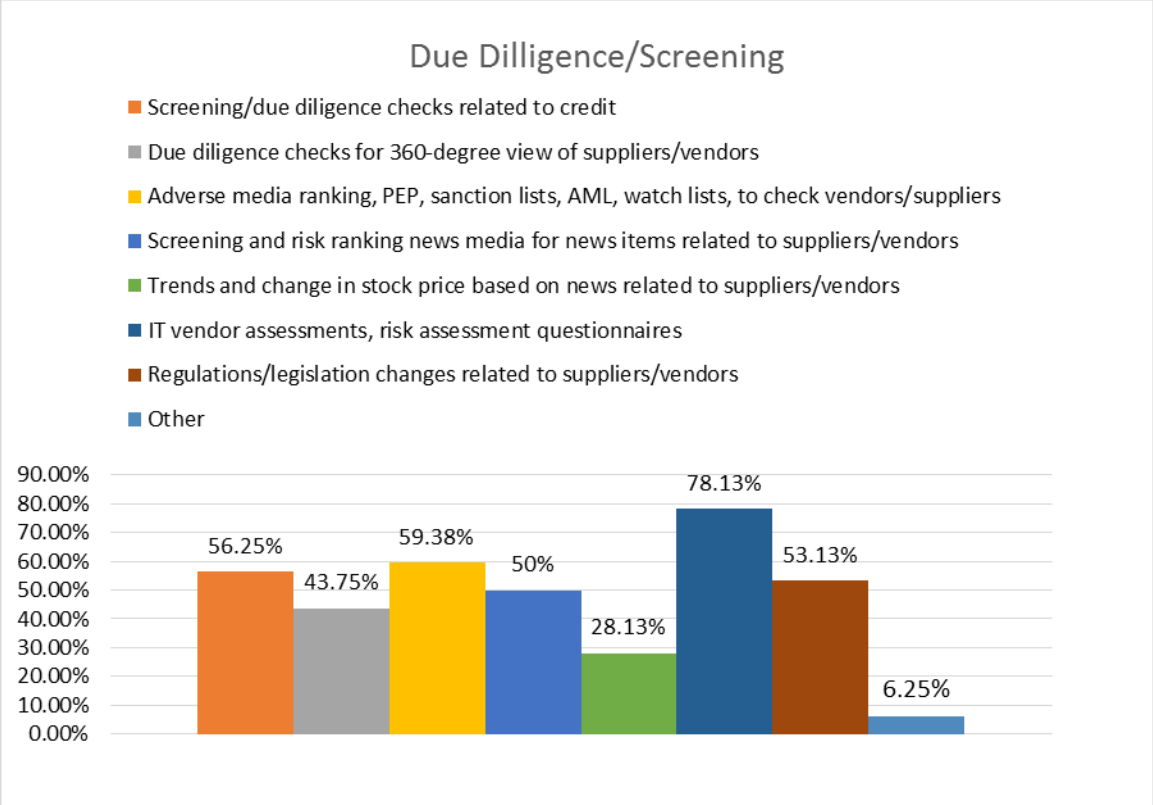
The data also shows an upward trend related to requiring an exit strategy for critical supplier, likely in response to FFIEC's Appendix J on business continuity management. For years 2014, 2015, and 2017, the percentage of institutions requiring exit strategies was 55%, 39%, and 67%, respectively.

Tools and Technology

Technology adoption varies across institutions. NContracts is a preferable third-party solution provider used by community banks (20%). Some other commonly used programs include Conetrix (Tandem) and Fortrex. Consistentwith past years' data, we have noticed high usage of MS Office programs and Homegrown programs. In the 2015 survey, 42% of participating institutions were using MS Access and Excel to manage their third-party risk management programs. The number of those who use the MS Office program decreased to 17% and the number of Homegrown systems increased from 4% in 2015 to 25% in 2017. When asked if institutions use the same primary technology to manage activities, documentation, and reporting for non-vendor third-party risk management programs, 56% of respondents selected "Yes."

Most institutions acquire data from third parties like LexisNexis, Dunn and Bradstreet, and Moody's to support due diligence and monitoring activities. The use of automated data feeds, automated alerts, and independent due diligence is an emerging practice, and most of the data comes from sources such as LexisNexis, Dunn and Bradstreet, and Moody's.

The most common types of due diligence that institutions use and/or are interested in obtaining are (1) IT vendor assessments/risk assessment questionnaires, (2) adverse media ranking/PEP/sanction lists/AML/watch lists, (3) screening/due diligence checks related to credit, and (4) regulations/legislation changes related to suppliers/vendors.



About 32% of respondents require cyber liability insurance from third parties that have access to personal and private information. About 40% of respondents indicated that their institution is has their own policy in place.

Contracts

About 57% of institutions use standard contract and risk control clauses for third-party relationships. This number is similar to year 2015 where 46% of respondents indicated they've implemented these standards. Standard contracts for vendors in 2014 were used by 19% of respondents.

Internal audit (50%), followed by ERM/ORM (30%), continues to play a key role in terms of conducting independent reviews of a third-party risk management program.

When it comes to the "Supplier Code of Conduct," 84% of respondents still do not have one in place. This is down from the 93% threshold noted in the 2014 data.

When asked about managing and reporting on third-party risk incidents and issues, consistently across the years, the top three responses were (in order from highest to lowest):

1. Escalates risk incidents and issues to the business line, the company's risk subject matter experts, and upper management.
2. Reports risk incidents and issues to the company's operational and management committees.
3. Reports risk incidents and issues in real-time, reports always available to management, and procurement/sourcing.

We asked our members about outsourcing. Currently, 92% of institutions do not outsource any part of sourcing, procurement, or supplier risk management. Also 54% answered that none of their due diligence assessments have been outsourced to third-party providers.

Regulatory and Compliance

In most cases, the Enterprise/Operational Risk Management (61%), or the regulatory liaison (18%) are responsible for identifying, tracking, and communicating regulatory and compliance updates/changes related to third-party risk management.

Approximately 47% of institutions have a risk oversight committee, formed specifically to oversee third-party risks. This is a decrease from 64% noted in 2015.

The following information about regulatory criticism can be used as a guide for program evolution across the sector. Please refer to question 48 for additional information.

Response	Percent
Completeness: program doesn't address full lifecycle of "vendor" third-party relationships	9.09%
Completeness: program doesn't include all critical "non-vendor" third-party relationships and activities	13.64%
Consistency: program is not applied consistently across all lines of business	4.55%
Business continuity/resilience (new Appendix J to FFIEC guidance)	18.18%
Cloud computing	4.55%
Governance and oversight	9.09%
Controls	4.55%
Effective Challenge	9.09%
Monitoring	13.64%

Response	Percent
Reporting	9.09%
Independent reviews	9.09%
Cybersecurity (e.g., horizontal Fed/OCC cyber review)	4.55%
Other (please specify)	40.9%

Fourth Parties

The final section of the survey was dedicated to fourth parties. There is a range of practices when it comes to how **material** fourth parties are identified.

- 44% require their third party to identify fourth parties during RFP process.
- 26% indicated that material fourth parties are identified in the contract.
- 17% selected "Other" and provided their processes for identifying material fourth parties.

In 2014, 29% of those surveyed confirmed that they perform due diligence on fourth parties, while 70% do not. This is consistent with our 2017 data (23% versus 64%). It is worth mentioning that this year participants could select "Partially," in addition to "Yes/No" choices.

Insights

Please see the following pages for detailed responses and examples of the range of practices institutions with asset sizes up $10 billion employ for third-party/vendor risk management.

Thank you to RMA member banks for contributing to this benchmarking study. The full report is available to those institutions that contributed to the study.